outputting the digital signature to the information device.

REMARKS

A Petition for Extension of Time pursuant to 37 CFR §1.136 and the fee required by 37 CFR §1.17(a)(3) are submitted herewith. The due date for response to the Official Action mailed February 28, 2001 is now August 28, 2001.

Regarding paragraph 2 of the DETAILED ACTION, the required corrected amendment to claim 27 has been made herein.

In paragraphs 6 and 7 of the DETAILED ACTION, claims 1-20, 26 and 27 were rejected under 35 U.S.C. §103(a) as being unpatentable over the previously cite publication of Friedman in view of the newly cited U.S. Patent No. 5,157,726 to Merkle et al.

Independent claims 1, 6, 10, 14, 26 and 27 as amended patentably distinguish the subject invention from the cited references.

Specifically, independent claim 1 specifies:

"c) means for using said software to generate a digital signature based upon the first information and the secret key information".

The significance of this is that the digital signature forms part of the information itself and is not merely attached to the information. Thus, in order to verify that the information is authentic, the receiver need merely check the decoded information itself to ascertain whether it is recognizable or not. It is not necessary to decode an attachment to the information and separately verify the attachment.

Turning now to the cited references, the publication to Friedman fails to show the generation of a digital signature from a part of the image signals as claimed by applicant. Friedman shows in Fig. 2, the generation of a hashing function. While this hashing function is

derived from the image signal it is kept separate from the image signal; and the private key which is used for the generation of the digital signature is applied only to the hashing function and not to the image signal itself. In fact, Friedman is careful to emphasize that the original message is untouched (Page 906, Col. 2, lines 4-7). Thus Friedman does not use the secret key to encode any part of the original image signal.

The cited patent to Merkle et al. also fails to disclose the formation of a digital signature by using a secret key to encode at least part of the message being sent. Instead, Merkle et al. attach a separately generated digital signature to a document to be authenticated. As can be seen in Fig. 3 of Merkle et al. a document to be provided with a digital signature is digitized at 56; and it is thereafter encrypted at 57. In parallel with this, a digital signature is generated at 62. This digital signature is then attached to or merged with the previously encrypted document. The digital signature itself does not form part of the encrypted document as in the present invention. Instead Merkle et al.'s digital signature is attached to or merged with the document.

Since neither Friedman's nor Merkle et al.'s disclosure provides any indication of applying a secret key to encode at least part of a document, no combination of these references is capable of anticipating or suggesting applicant's claimed information input device in which a document is provided with a digital signature by encoding at least a portion of the document with the sender's secret key.

In view of the foregoing, it is submitted that claim 1, as amended, patentably distinguishes over Friedman and Merkle et al. considered both individually and in combination.

Independent claim 6 specifies:

"d) means for using said software to generate a distinguishing information based on the secret information and the information compressed by said compressing means".

- 7 -

Independent claim 10 specifies:

"d) an operation device for carrying out an operation using said software, the image data and the secret information to produce a digital signature"; and

Independent claim 14 specifies:

"c) an operator for executing a command based on said algorithm for generating a digital signature by using the image data and the secret key information"; and

Claim 26, as now amended, specifies:

"c) a step of using said software to generate a digital signature based upon the first information and the received secret key information";

Claim 27, as now amended, specifies:

"(c) a step of using said software to generate a digital signature based upon the first information and the secret key information received from the external device".

Thus, it will be seen that each of applicant's independent claims 1, 6, 10, 14, 26 and 27 specify that at least a portion of the image data that is to be sent is encoded with a secret key so that the image itself or a portion thereof forms part of the digital signature. Since neither Friedman nor Merkle et al. provide any indication of the encoding of the image data itself with the user's secret code, it is submitted that neither of these references, nor their combination, is capable of anticipating or making applicant's claims 6, 10, 14, 26 or 27 obvious. Accordingly, it is submitted that these claims patentably distinguish over the references and are allowable.

Claims 2-5, 7-9, 11-13 and 14-20, are each dependent on one or more of the independent claims discussed above and accordingly these claims are patentable over the references for the same reasons given above in regard to the independent claims. Moreover the specific structures and methods defined by these dependent claims provide additional novelty as well as

- 8 -

additional advantages which can be appreciated from the specification. For these reasons also, claims 2-5, 7-9, 11-13 and 14-20 patentably distinguish over the references and are allowable.

New claims 28-30 have been added to provide a further measure of protection for the subject invention. These claims also distinguish over the references in that they provide for generating a digital signature on received digital data by encoding a part of the data itself with a secret key.

Independent claim 28 specifies:

"processing means for generating said digital signature based on said digital data, said secret key and said software".

Claim 29 is dependent on claim 28 and incorporates the same distinguishing limitation.

Independent claim 30 specifies:

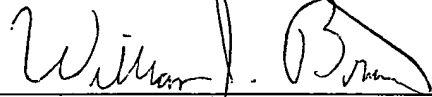"generating said digital signature based on said digital data, said secret key and said software".

Thus, each of claims 28-30 also specify the step of, or apparatus for, generating a digital signature by use of the information itself to which the digital signature applies. As explained above, the references generate a digital signature using other information and then attach the digital signature to the document. The references give no suggestion of using the information itself to generate the digital signature.

It is submitted, in view of the foregoing, that this application is now in condition for allowance. Further consideration by the Examiner and allowance of this application is

respectfully requested.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,

William J. Brunet
Attorney for Applicants
Registration No. 20,452

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200
NYMAIN#195387V1

VERSION WITH MARKINGS TO SHOW CHANGES TO CLAIMS

1.   (three times amended) In an information input device, the combination

of:

a) means for inputting first information;

b) means for receiving secret key information and software for generating a

digital signature from an external device and for storing such received secret key information and

said software, said secret key information being the secret key of a person using the information

input device;

c) means for using said software to generate[generating] a digital signature

based upon the first information and the secret key information; and

d) means for outputting said first information containing said digital signature,

        whereby the output information is provided with the digital signature of the

person who uses the information input device.

6.   (three times amended) An information input device REOEIVED

a) means for inputting first information;   AUG 2 9 2001

b) means for compressing said first information;   Group 2100

c) means for receiving secret key information and software for generating a

digital signature from an external device and for storing said received secret key information and said

software, said secret key information being the secret key of a person using the information input

device;

-i-

d) means for using said software to generate[generating] a distinguishing

information based on the secret information and the information compressed by said compressing

means and

e) means for outputting said first information containing said digital signature,

wherein said external device stores the secret key corresponding to a registered

user; and

whereby the output information is provided with the digital signature of the

person who uses the information input device.

10.   (three times amended) An image input apparatus comprising:

a) an image input device for inputting said image data;

b) means for receiving secret key information and software for generating a

digital signature based on said secret key information from an external device;

c) a memory for storing said software and said secret key information which is

received from said external device[and received from the external device], said secret key

information being the secret key of a person using the information input device;

d) an operation device for carrying out an operation using said software, the

image data and the secret information to produce a digital signature; and

e) means for outputting said first information containing said digital signature,

whereby the output information is provided with the digital signature of the

person who uses the information input device.

14.   (three times amended) In an image input system:

a) a first terminal device for inputting image data;

b) a second terminal device for receiving secret key information from an

external device and an algorithm for generating a digital signature, said second terminal device [

and] having a memory for storing said received secret key information, said secret key information

being information which corresponds to a user;

c) an operator for executing a command based on said[an] algorithm for

generating a digital signature by using the image data and the secret key information; and

d) means for outputting said first information containing said digital signature,

whereby the output information is provided with the digital signature of the

person who uses the information input device.

26.   (three times amended) An information input method comprising:

a) a step of inputting first information into an information input device;

b) a step of receiving secret key information and software for generating a

digital signature from an external device and for storing the received secret key information and said

software, said secret key information being the secret key of a person using the information input

device;

c) a step of using said software to generate[generating] a digital signature based

upon the first information and the received secret key information; and

d) outputting said first information containing said digital signature,

whereby the output information is provided with the digital signature of the

-iii-

person who uses the information input device.

      27.   (three times amended) A computer readable memory programmed to cooperate[which cooperates] with a data processor and an information input unit to carry out:

      (a) a step of inputting first information into an information input device;

      (b) a step of receiving secret key information and software for generating a digital signature from an external device and storing the received secret key information and said software, said secret key information being the secret key of a person using the information input device;

      (c) a step of using said software to generate[generating] a digital signature based upon the first information and the secret key information received from the external device; and

      d) outputting said first information containing said digital signature,

      whereby the output information is provided with the digital signature of the person who uses the information input device.